Department of Homeland Security
National Infrastructure Protection Center
Daily Open Source Infrastructure Report
for 19 March 2003

Current Nationwide Threat Level is

HIGH
High Risk of Terrorist Attacks

For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Government Accounting Office has published a report entitled "Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities but the Extent of Security Preparedness Is Unknown." (See item 8)
- Federal Computer Week reports a hacker last week exploited a previously unknown vulnerability in Microsoft Corp.'s Windows 2000 operating system to gain control of an Army Web server; Microsoft has developed a patch, available on the Microsoft Web site, to fix it. (See item 33)
- CNET News.com reports the open−source community is urging customers to patch their systems to close a hole in a software component known as Samba, which is found on many workstations and servers running any one of the variety of flavors of Linux and Unix, including systems running Apple OS X. (See item 35)
- eWEEK reports officials at the CERT Coordination Center are monitoring at least five large networks of compromised machines installed with so−called bots, that can connect compromised PCs or servers to Internet Relay Chat servers, which attackers commonly use to execute commands on the remote systems. (See item 36)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: High, Cyber: High
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *March 18, Platts Global Energy News* — **Saudis have stockpiled 50−mil bbl of oil . Saudi Arabia has stockpiled nearly 50−mil bbl of oil which it will use if war disrupts Iraqi exports, the New York Times reported Tuesday. "We have about 50−mil bbl, most of it in the country," the paper quoted a senior unnamed Saudi official as saying. "We can tap into it immediately once there is a shortfall."** Saudi Arabia has been boosting its crude production steadily since early December, when a strike paralyzed Venezuelan oil production and exports. Former Saudi oil minister Zaki Yamani's London−based think−tank the Center for Global Energy Studies said Monday that key producers, including Saudi Arabia, were stockpiling oil ahead of the possible loss of Iraqi supplies.
   Source: http://www.platts.com/stories/home3.html

2. *March 17, Reuters* — **Top California power regulator touts grid master plan. California, for the first time, is forging a single plan to guard against the blackouts and price spikes that battered it during the 2000− 2001 energy crisis, the state's top regulator said.** "California has aimed before to upgrade the power system, but this is the first time that state agencies have committed to work together on a single plan," Michael Peevey, the new president of the California Public Utilities Commission (CPUC), said in an interview with Reuters. **Peevey said California plans to cut consumer demand through aggressive conservation programs, build up to 2,000 megawatts of new plant capacity a year and add renewable energy to strengthen supplies −− power for 2 million homes.** California's energy future, outlined in the plan drafted by the CPUC and two other power agencies, also will feature small generating plants in neighborhoods where the energy is used, a revamped power grid and new pipelines to import natural gas.
   Source: http://www.energycentral.com/sections/news/nw_article.cfm?id =3716020

3. *March 17, Omaha World−Herald* — **Coal, rail contracts hold key to power rates. Officials with the Omaha Public Power District are painstakingly laying the foundation for one of the board's most important decisions, one that will have a significant impact on customer rates.** This summer, the board will vote on a batch of coal and rail contracts valued at about $225 million. Together, the contracts will provide coal to OPPD's two largest power plants for the five years from 2004 through 2008. **OPPD Chief Executive Officer Fred Petersen credits the current coal and rail contracts with playing a key role in keeping electric rates low. "It's one of the reasons we've been so successful over the last five years," he said.** OPPD's rates are 18 percent to 20 percent below the national average, said spokesman Jeff Hanson, and Power Magazine has ranked the utility's Nebraska City plant as the third most affordably run coal plant in the country. The decision the board faces is complicated because it could involve up to 50 bidders on various contracts.
   Source: http://www.energycentral.com/sections/news/nw_article.cfm?id =3715717

4. *March 17, BBC* — **Numerous errors found in Japanese nuclear power plant safety reports. More than 100 errors have been found in safety inspection reports on a nuclear power plant run by Chubu Electric Power Co., but the company has denied any irregularities.** The errors, which include wrong numbers and reference codes related to plant operations, were found in the records of about 2,500 safety checks that Chubu Electric conducted over the last 10

years at four reactors at the Hamaoka nuclear station in Shizuoka Prefecture, a company official said Monday. **The official, who asked not to be named, described the errors as "clerical" and said they will be reported shortly to the Nuclear and Industrial Safety Agency of the Ministry of Economy, Trade and Industry.** Since last September, Chubu Electric has cross−checked its own records with those kept by the subcontractor engaged in safety inspections on the plant, following revelations last August that Tokyo Electric Power Co. had falsified safety reports to cover up defects at its nuclear facilities. The Chubu Electric official said the errors, 16 of which had already been made public in an interim report released last fall, occurred when reprinting the subcontractor's data in the company's own books.
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id =3716059

5. *March 17, Environment &Energy Daily* — **New security guidelines for power plants probed. A closed hearing in the House Energy and Commerce Oversight and Investigations Subcommittee Tuesday (March 18) will look at the Nuclear Regulatory Commission's progress at revising the Design Basis Threat (DBT), or the level of attack for which plants have to be prepared.** Since the terrorist attacks of 2001, the commission has been reviewing the security guidelines to consider the new level of threat the power plants face. The Nuclear Regulatory Commission (NRC) regional administrator Hubert Miller said at House hearings earlier this month that the commission could be finalizing the new guidelines **Specifics on the DBT are safeguarded, but NRC has said publicly it requires at least the ability to fend off a group of attackers with some inside information about the plant.** Anti−nuclear interest groups and some lawmakers have called for specific items they want to see in a new DBT. House Energy and Commerce ranking member John Dingell (D−Mich.) along with fellow committee member Edward Markey (D−Mass.) sent a letter to the General Accounting Office early last year calling for an investigation on the regulations. A GAO spokeswoman said the report, with the working title "Nature and adequacies of security policies and procedures and entities licensed by NRC," could be complete by June 30.
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=eenews_2003_03_17_eng−eenews_energy_eng−eenews_energy_124555_7804589184142294842a>

6. *March 16, BBC* — **Chernobyl shell in poor condition − Ukraine's nuclear regulator . The Chernobyl nuclear power plant still poses a potential threat as the sarcophagus over the ill−fated No 4 reactor is deteriorating, the head of Ukraine's state committee for nuclear regulation, Vadym Hryshchenko, has said.** Ukraine's imperfect legislation hampers the repairs. Kiev has been working to bring its nuclear regulation in line with common European standards in order to meet the EU membership requirements. Hryshchenko's interview with Mykola Petrushenko published in the Uryadovyy Kuryer government newspaper on 13 March; subheadings inserted editorially is available at the url below.
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id =3716052

[Return to top]

Chemical Sector

7. *March 18, The Times (Trenton, NJ)* — **Chemical site safety upgrades proposed. New Jersey chemical companies would be required to prepare disaster prevention plans for reactive**

chemicals under Governor McGreevey administration's proposal that would significantly expand the list of materials covered by the state's Toxic Catastrophe Prevention Act. The proposed regulations would add 30 substances to the current list of well over 100 chemicals. Reactive chemicals are not considered hazardous in isolation but become dangerous when mixed with other substances, such as air, water or other chemicals. **Under the rules, companies that use such chemicals would be required to develop a plan to protect the facility from potentially dangerous reactions. Such a plan might include installing cut−off valves or making sure the reactive chemical is kept isolated.** Sodium hydrosulfite, which caused a fatal explosion at Lodi−based Napp Technologies in 1995 when it mixed with aluminum powder, is one of the chemicals proposed for the list. Reactive chemicals are not covered by federal regulation. Bradley Campbell, commissioner of the state Department of Environmental Regulation, called the omission "a significant loophole in the law that has left communities at risk." Representatives of the chemical industry call the proposed changes in the regulations a needless and costly expansion in troubled economic times.
Source: http://www.nj.com/statehouse/times/index.ssf?/base/news−0/10 47985226214243.xml

8. *March 14, Government Accounting Office* — **Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities but the Extent of Security Preparedness Is Unknown. The Government Accounting Office published Report GAO−03−439 on March 14, which discusses the security preparedness at chemical facilities.** The events of September 11, 2001 triggered a national re−examination of the security of thousands of industrial facilities that use or store hazardous chemicals in quantities that could potentially put large numbers of Americans at risk of serious injury or death in the event of a terrorist−caused chemical release. GAO was asked to examine available information on the threats and risks from terrorism, federal requirements for security preparedness, actions taken by federal agencies to access the vulnerability of the industry and voluntary actions taken by the chemical industry concerning security preparedness. **GAO recommends the Secretary of Homeland Security and the Administrator of the Environmental protection Agency jointly develop a comprehensive national chemical security strategy that is both practice and cost effective, which includes assessing vulnerabilities and enhancing security preparedness.** Report highlights: http://www.gao.gov/highlights/d03439high.pdf
Source: http://www.gao.gov/new.items/d03439r.pdf

[Return to top]

Defense Industrial Base Sector

9. *March 17, Associated Press* — **Battelle opens $22M research center.** A federal government contractor opened a center Monday in Harford County to develop devices to detect chemical and biological weapons in the air, on the ground and inside buildings. **Battelle Memorial Institute, a national nonprofit research company based in Columbus, Ohio, built the $22 million laboratory and office complex near one of its largest clients, the Army's Aberdeen Proving Ground.** Defense against biological and chemical weapons has become a government spending priority since the Sept. 11 terrorist attacks and the anthrax mail attacks in the autumn of 2001. "We have been doing this for more than a decade; it is only now that the importance of this research is really coming into the limelight," said Stephen E. Kelly, senior vice president and general manager of defense systems at Battelle, which conducts more than $2 billion in

annual research and development. **The Defense Department spent $402.4 million last year on its chemical−biological defense program, and has requested $1.374 billion for fiscal 2003, according to the program's annual report.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A43121−2003Mar 18.html

10. *March 17, Government Computer News* — **DISA consolidation will cut 1,200 jobs.** The Defense Information Systems Agency has announced a plan to consolidate its Computing Services Directorate over the next 30 months, which may result in the loss of up to 1,200 jobs. Computing Services, responsible for combat support data processing, currently operates six mainframe processing sites running IBM OS/390 and Unisys systems. **The consolidation would reduce the number to four sites, DISA officials said in a press announcement last week. The directorate employs 2,300. DISA will also consolidate its system management functions into four locations, according to Robert Bryant, an agency spokesman. Concurrently, the agency is setting up data mirroring and replication centers at separate sites to prevent catastrophic loss of data and to minimize the risks of data center consolidation, Bryant said.**
Source: http://www.gcn.com/vol1_no1/dod/21409−1.html

[Return to top]

Banking and Finance Sector

11. *March 19, CNN* — **Treasury fortifies markets; Government takes steps to keep money flowing, and IRS working, in heightened state of alert .** The Treasury Department said Tuesday it is taking steps to protect U.S. financial markets from potential terrorist attacks during an imminent war with Iraq. **Treasury said it was arranging for protection of markets by National Guard troops, giving high−tech communication equipment to regulators and "critical" financial institutions, and taking other steps to keep money flowing once war starts. "The financial markets are the engine of our free enterprise economy," the department said. "At Treasury, we are determined that the financial markets continue to conduct business even during times of hostilities abroad or adversity at home."** Citing "operational security," Treasury wouldn't give precise details about the steps it is taking but said it had identified the most critical financial institutions and had arranged for experts to inspect those institutions for vulnerable spots. Treasury also noted that private firms had helped by improving "business continuity" plans and establishing new backup facilities in remote locations. Treasury fact sheet: http://www.treasury.gov/press/releases/sheet.htm
Source: http://money.cnn.com/2003/03/18/news/treasury/

12. *March 18, Washington Post* — **Markets, brokerages brace for volatility.** Wall Street moved onto a war footing on Tuesday as stock exchanges and brokerage firms prepared for possibly volatile trading days to come. **Officials at the New York Stock Exchange and the Nasdaq Stock Market said they had plans in place to handle chaotic wartime trading and to keep markets running in the event of any domestic terror attacks sparked by a U.S.−led effort to oust Iraqi leader Saddam Hussein.** At the NYSE, officials said they were confident they could easily handle any massive war rallies or sell−offs. The stock exchange is capable of handling five times the current average daily trading volume, a spokesman said. Nasdaq officials also said their systems could handle large volume increases. Both the NYSE and

Nasdaq established emergency procedures after the Sept. 11, 2001, attacks on the World Trade Center and the Pentagon to try to prevent terrorists from disrupting trading. **New York Stock Exchange officials said they have established a backup trading floor and duplicate computer systems that would prevent any breakdown in the flow of information from brokerage firms to the floor. Such a breakdown was a key reason the NYSE remained closed for four days after Sept. 11. Nasdaq officials also said their post−Sept. 11 decision to duplicate trading technology would make it virtually impossible for terrorists to interrupt operations.** For security reasons, officials at Nasdaq and the NYSE declined to provide details of their plans.
Source: http://www.washingtonpost.com/wp−dyn/articles/A42443−2003Mar 17.html

13. *March 17, Associated Press* — **Property owners facing high prices for terrorism insurance.** High prices for terrorism insurance are causing major problems for commercial property owners, who are having to obtain the coverage before receiving approval for loans. Federal law requires insurance companies to offer coverage for terrorist attacks, but officials failed to set rate standards. The result has been widely varying prices, according to property management groups and insurance brokers. **"This is a real crisis for property owners," said Scott Adams, director of corporate insurance and risk management for Insignia/ESG, a national commercial real estate services provider.** "Major commercial (property) owners can't afford it," Adams said. "You are in fact seeing property owners in places like Connecticut, upstate New York and New Jersey who are not purchasing terrorism insurance." **Some property owners may decline the insurance, but lending institutions could demand terrorism coverage as a condition of a mortgage.** Buildings near a monument or major metropolitan area, or those that house government agencies or foreign−based companies, are receiving more scrutiny and higher rates by insurance companies.
Source: http://www.newsday.com/news/local/wire/ny−bc−ct−−terrorismin suranc0317mar17,0,5768600.story?coll=ny−ap−regional−wire

[Return to top]

Transportation Sector

14. *March 18, CNN* — **Ridge outlines enhanced security plan: tighter security at airports, ports, rail stations.** With the terror threat alert level raised from yellow to orange, Homeland Security Secretary Tom Ridge on Tuesday outlined a plan to enhance security nationwide. "Your federal government is ready," Ridge told reporters at a briefing, at which he raised anew the possibility of terrorist attacks against the United States. Ridge said tighter security at airports, rail stations and ports is part of what has been dubbed Operation Liberty Shield. Border protection and increased security at airports and railways, and greater road security are also planned. **Homeland Security called for temporary flight restrictions over certain U.S. cities, including Washington and New York**, though the Federal Aviation Administration told CNN it had not yet issued those rules. **The TSA is ordering airports to conduct random inspections of vehicles, increase canine patrols, and increase the overall law enforcement presence in and around airports. The agency will also be putting up temporary signs inside airports asking the public to be aware of the increased threat level and to report unattended bags and suspicious behavior.** More details on Operation Liberty Shield can be found at http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0115.xml

Source: http://www.cnn.com/2003/US/03/18/sprj.irq.terror.alert/

15. *March 18, Federal Motor Carrier Safety Administration* — **Anti−terrorism tips for hazardous materials drivers.** The Federal Motor Carrier Safety Administration (FMCSA) has issued anti−terrorism tips to truckers who transport hazardous materials. The FMCSA recommends that certain protective activities be undertaken when the National Threat Level is raised to Code Orange. **While on the road, drivers should remain alert; look for vehicles following them; be aware of any possible surveillance of their facility or truck; refrain from discussing cargo, destination, or trip details; and maintain functioning communication devices.** In addition, the FMCSA issued guidelines for safety while stopping at facilities and for protecting hazmat vehicles.
Source: http://www.fmcsa.dot.gov/Home_Files/hmdatt.htm

16. *March 18, Reuters* — **War may hurt airlines, government to help. The U.S. government acknowledged on Tuesday that a war with Iraq could hurt the nation's airlines and said it was ready to move quickly with assistance measures if necessary.** "We will be ready to move very quickly if the need arises," Transportation Secretary Norman Mineta told the Federal Aviation Administration's annual forecast conference. With a U.S.−led invasion of Iraq seen just days or even hours away, the FAA offered an assessment more understated than the alarming scenario delivered by the industry last week, **but it still saw war as one of the "greatest risks" to recovery.** On Capitol Hill, Congressman James Oberstar, a Minnesota Democrat, **plans on Wednesday to introduce an airline aid bill that includes federal loan guarantees to cover rising fuel prices.** The leading association for the major U.S. airlines said last week that **an Iraq war lasting 90 days could drive the industry's annual losses to $10.7 billion, force more bankruptcies and cost 70,000 jobs.**
Source: http://reuters.com/newsArticle.jhtml?type=businessNewsID=2402106a>

17. *March 17, Federal Computer Week* — **Slow going on border systems, officials say. Homeland Security Department (DHS) officials said they will likely meet the Dec. 31 deadline for completing the automated system to track the entry and exit of visitors to the United States at airports and seaports, but may have a hard time meeting the 2005 deadline for land ports.** Installing the entry/exit system at land ports of entry would require infrastructure improvements. And the addition of biometric technologies, such as fingerprint readers and iris scanners, complicates the system. **Immigration officials are required to have the system running at the nation's 50 largest land ports by the end of 2004 and all land ports by the end of 2005. The system will ultimately improve access to relevant information about visa eligibility, help detect fraudulent documents, process biometric data for exact traveler information and improve information sharing among agencies.** Testifying at a joint hearing of two Senate Judiciary subcommittees on border technology March 12, Asa Hutchinson, DHS undersecretary for border and transportation security, said he believes the department will make the first deadline. Although technology used to secure the nation's borders has progressed substantially, there is still much work to be done, he said. "Technology is a critical tool that enables hard−working men and women of the Department of Homeland Security to properly balance our national security imperative with the free flow of goods and people across our nation's borders," Hutchinson said at the hearing.
Source: http://www.fcw.com/fcw/articles/2003/0317/news−border−03−17− 03.asp

[Return to top]

Postal and Shipping Sector

18. *March 18, The Oregonian* — **Defensive mode deals change on a big scale to Seattle waters.** Puget Sound looks like the same scenic, bustling inland waterway it was before Sept. 11, 2001, but for the people who do business on the sound −− or for those charged with securing it from terrorists −− it's a brand new body of water. **Now, container ships must give four days' warning that they're coming, specify what they're carrying, then subject their cargo to gamma ray imaging and radiation checks. All ferry passengers must get off at each stop while the boats are swept for suspicious packages.** When the Coast Guard boards vessels it looks for terrorists and bombs. Its new Marines−trained unit patrols the sound in fast, bulletproof boats with 50−caliber machine guns. **Security changes have hit the Columbia River, too, but they are not as dramatic as Puget Sound's because there aren't nearly as many foreign ships or potential terrorist targets to worry about. A February study by a national insurance advisory group ranked Seattle among the nine U.S. cities most likely to be attacked.** Some reasons for the ranking include Seattle's downtown population density in skyscrapers and stadiums as well as its proximity to the Canadian border, where one bomb−toting al−Qaeda terrorist was caught with plans to sleep near the Space Needle. **Puget Sound also is the nation's third−busiest trade waterway and home to the country's largest ferry fleet**, which packs almost as many riders onto its biggest boats as died in the World Trade Center attack. **Charles Mandigo, special agent in charge of the Seattle FBI office, also notes the unsettling fact that photographs of Seattle −− including shots of its waterfront −− popped up on a computer found in an al−Qaeda hide−out in Afghanistan.**
Source: http://www.oregonlive.com/news/oregonian/index.ssf?/base/front_page/1047996057180700.xml

19. *March 17, KRON* — **Security high at Port of Oakland.** Security remains high at the Port of Oakland as the nation strides closer to war. **The port has been listed as one of the nation's top terror targets due to its economic importance.** "The port of Oakland is the 4th largest port in the nation," says Harold Jones of the Port of Oakland. **He says the port is listed as America's number two terror target. "That's not an assessment of the port's vulnerability, but more on the impact it would have**," Jones says. **That impact goes well beyond the Bay Area.** Jones displayed two thick binders listing companies nationwide that export or import through the Port of Oakland. **So it's not just the port's 44,000 local workers to think about, its jobs nationwide, even California farmers and exports.**
Source: http://www.kron4.com/Global/story.asp?S=1184050

[Return to top]

Agriculture Sector

20. *March 18, San Bernardino Sun* — **Exotic Newcastle disease found at two San Bernardino chicken ranches. California officials killed 48,750 birds at a Chino ranch after identifying Exotic Newcastle disease there on Friday, California Department of Food and Agriculture**

spokesman Larry Cooper said. On Monday morning, officials also confirmed the disease at a second San Bernardino County ranch the 20th Southern California ranch infected by Exotic Newcastle disease since late December. Cooper estimated roughly 50,000 birds will be killed there. Euthanization is also under way at a 4,000−bird ranch in San Diego County where exotic Newcastle was identified Friday, Cooper said. Citing biosecurity concerns, officials are not releasing names or locations of infected ranches whose chickens have not yet all been killed. But Cooper said both sites are within the quarantine area, not far from previously−infected ranches.
Source: http://www.sbsun.com/Stories/0,1413,208~12588~1251514,00.htm l

[Return to top]

Food Sector

21. *March 18, Food Ingredients First* — **National food safety program launched. The first comprehensive food safety training program designed specifically for retail food stores nationwide was launched Monday at the Food Safety Summit Meeting in Washington, D.C., by researchers from Purdue and Indiana universities who developed the program.** Richard Linton, Purdue food science professor, and David McSwane, IU associate professor of public and environmental affairs collaborated to write a textbook and training program for managers and workers in grocery stores, supermarkets, convenience stores, superstores, and any retail store that sells food to consumers. **"This training program for the retail food store industry is important because many states require that at least one person from each food establishment must pass a nationally recognized food safety certification exam," Linton said. "This is a major step in having uniform training to ensure food safety."** The authors used the Food and Drug Administration Model Food Code as a basis for the main text.
Source: http://www.foodingredientsfirst.com/newsmaker_article.asp?id NewsMaker=3082/font>

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

22. *March 18, BBC News* — **Modelers say thousands would die in anthrax attack. An anthrax weapon aimed at a major city could kill at least 123,000 people even if every victim received treatment, experts have calculated.** U.S. researchers have used a computer model to predict the devastation that would result from the launch of an anthrax bomb or missile on a city the size of New York. **The figures are based on what would happen if a bomb containing one kilogram of anthrax spores was dropped on a city of 10 million inhabitants.** The projected number of fatalities is based on the assumption that antibiotics would not be administered for 48 hours until the first symptoms appeared. **If it proved possible**

to distribute drugs more quickly, then the death toll could be substantially reduced.
Source: http://news.bbc.co.uk/1/hi/health/2857207.stm

23. *March 18, San Francisco Chronicle* — **Mysterious illness may be new disease. A mysterious, flulike illness that has stricken scores of hospital workers in Southeast Asia has stumped a battery of tests for known bacteria and viruses and most likely represents a new human disease of unknown origin, federal health authorities said Monday. At least 14 cases bearing some resemblance to the illness are being evaluated in the United States.** Under prodding by the United Nations' health agency, China has disclosed an outbreak of 305 cases from November through February that appear similar to severe acute respiratory syndrome (SARS). There were five deaths in China, but none of the cases are included yet in the official World Health Organization (WHO) count. **Centers for Disease Control and Prevention Director Dr. Julie Gerberding told reporters that 10 of the 14 suspected cases in the United States were "almost certainly not" SARS, but that "it would not be surprising" to find the illness soon in the U.S.** Gerberding said she was confident that laboratories in the United States or in eight other nations testing for the disease would pinpoint its cause. But the disease detectives are now fairly sure it is a bug they haven't encountered before.
Source: http://www.sfgate.com/cgi−bin/article.cgi?file=/c/a/2003/03/ 18/MN253862.DTL

24. *March 18, New York Times* — **Health organization stepping up efforts to find cause of mysterious pneumonia. The World Health Organization (WHO) expanded its network of laboratories yesterday in an effort to find the cause of a mysterious respiratory illness that has spread with the aid of international plane travel from Asia to Canada and countries in Europe.** The agency is coordinating scientists from 11 laboratories in 10 countries to seek the cause of severe acute respiratory syndrome (SARS) which it says is a threat to world health. **So far scientists at five laboratories have failed to identify any known infectious agent as its cause. Dr. Julie L. Gerberding, the director of the U.S. Centers for Disease Control and Prevention (CDC) said scientists at her agency are focusing on either an unusual known infectious agent that is difficult to grow in a laboratory or on a novel agent.** WHO said that it has no scientific proof that the cases in the different countries are all the same disease. But the similarity in symptoms and epidemiologic characteristics have led officials to assume they are. Linking the cases will require identification of the agent causing SARS.
Source: http://www.nytimes.com/2003/03/18/health/18INFE.html

25. *March 18, Contra Costa Times* — **Kaiser warns on drug orders.** Kaiser Permanente announced Monday that any member of its Northern California health network taking a prescription dated March 13 on the bottle should immediately call their local pharmacy to make sure the label is correct. **A labeling problem prompted Kaiser to recall 4,700 refill prescriptions issued last Thursday and picked up either that day or Friday.** While most of the questionable prescriptions have been checked for errors, 152 people have not been reached. **An electronic malfunction caused potentially serious labeling errors at Kaiser Permanente's 108 Northern California pharmacies last week. Kaiser spokesperson Lea Rubio said the problem resulted from a power outage in the Southern California facility where its pharmacy system is located.**
Source: http://www.bayarea.com/mld/cctimes/5419097.htm

[Return to top]

Government Sector

26. *March 18, Washington Post* — **Federal agencies prepare for war.** As war looms in Iraq, federal agencies are girding against possible retaliatory attacks in Washington by honing protective measures put in place after the Sept. 11, 2001, terrorist strikes and adding a few new ones as well. Like most Americans, the agencies are getting some guidance from the administration. The color−coded Homeland Security Advisory System, for example, directs officials to take certain steps as the risk of an attack rises, such as increasing surveillance at buildings, dispersing workers to alternate sites and, in an extreme case, closing government facilities. **For the most part, however, each federal agency is on its own in crafting safety plans, training employees for an emergency and deciding whether to buy gas masks and other protective equipment. Much of the planning has taken place in secret, with officials saying that disclosing security measures −− even, in some cases, to employees −− would assist terrorists.** "[I]t is very likely that numerous steps have already been taken to secure your building that are not subject to open discussion," Kay Coles James, director of the Office of Personnel Management, wrote in a new eight−page federal employee emergency guide posted on OPM's Web site last week. "Trust your manager −− this information may be held more 'tightly' to better protect you from individuals who may seek to cause harm." The emergency guide can be found at http://www.opm.gov/emergency/PDF/EmployeesGuide.pdf
Source: http://www.washingtonpost.com/wp−dyn/articles/A42380−2003Mar 17.html

27. *March 18, Washington Post* — **U.S. heightens alert, asks for Guard call−ups.** The U.S. government raised its terrorist threat level to orange, or "high risk," on Tuesday night even as President Bush was delivering his speech on Iraq. Top federal officials, meanwhile, asked many of the 50 states to deploy the National Guard or state police to protect sensitive sites across the nation from possible attack. **While National Guard troops have periodically been assigned to patrol some airports and other facilities since Sept. 11, 2001, this is the first request for deployment of the units across such wide swaths of the country. They or state police contingents are expected to be assigned to patrol some railroads, bridges, chemical plants, nuclear facilities and other key infrastructure sites, officials said.** "The intelligence community believes that terrorists will attempt multiple attacks against U.S. and coalition targets worldwide in the event of a U.S.−led military campaign against Saddam Hussein," Homeland Security Secretary Tom Ridge said in a statement released last night. **Around the nation's capital, the District, Maryland and Virginia governments prepared to step up security and preparedness efforts behind the scenes, while bracing for the possibility of federal street closings downtown, the heightened presence of military patrols and restricted access to government sites.** State and District agencies stepped up law enforcement and intelligence activities and information−sharing with federal anti−terrorism investigators. District police prepared to activate their Joint Operations Command Center, which controls a network of surveillance cameras in the city. The District and state emergency management operations centers remained in standby mode.
Source: http://www.washingtonpost.com/wp−dyn/articles/A41737−2003Mar 17.html

28.

March 18, Washington Post — **Bill seeks to expand pool for national security jobs.** A recent survey found that only 24 percent of job seekers believe the best opportunities for an engineering career are in the government. The departments of State and Defense struggle to hire and keep science and technology experts. Numerous agencies are short of translators and interpreters. Six large agencies that were moved into the Department of Homeland Security could lose roughly a quarter to half of their employees to retirement during the next five years. **In an effort to strengthen the government's recruitment and retention in the areas of science, math and foreign languages, a bipartisan group of senators has introduced legislation to expand the existing student loan repayment program for national security agencies and create a job rotation program for mid−level employees holding national security jobs.** "Today, agencies are forced to decide between funding programs and investing in their workforce," Sen. Daniel K. Akaka (D−Hawaii) said. "This is a no−win situation and has prevented many agencies from fully utilizing the federal student loan repayment program, which is intended to be a powerful recruitment and retention tool." **Under his proposal, Akaka said, a fund would be set up in the Office of Personnel Management to repay student loans for employees in national security positions who agree to serve in the government for at least three years.** The legislation would create a pilot project to allow those employees to receive $10,000 in loan repayments per year, up to $80,000 in a lifetime. The current loan program, available to employees in all job categories, provides up to $6,000 per year and $40,000 total.
Source: http://www.washingtonpost.com/wp−dyn/articles/A42856−2003Mar 17.html

29. *March 18, Honolulu Advertiser* — **No added threat to Hawaii, Lingle says.** While the rest of the nation has raised its terror−alert level to orange or "high risk" on the eve of a likely invasion of Iraq, Hawaii will remain at a lower threat level, Gov. Linda Lingle said yesterday. **Lingle said state Adjutant General Robert Lee spoke with national homeland security officials and "after his conversation at this time there is no additional credible threat in the state of Hawaii and we will maintain our alert status at the blue level." The blue level, known as "guarded," is the second−lowest alert level.** The decision by Lingle to stay at the blue level comes as President Bush and Homeland Security Secretary Tom Ridge warned yesterday that the United States should expect a terrorist response in the event of military action in Iraq. **The amount of discretion left to the states in determining terror alert status is unclear. Lingle's spokesman, Russell Pang, said last night that state alert levels are left up to the discretion of the individual states.**
Source: http://the.honoluluadvertiser.com/article/2003/Mar/18/ln/ln0 4a.html

30. *March 18, Boston Globe* — **U.S. check leads to wave of firings.** A controversial program designed to clear up millions of erroneous Social Security numbers has resulted in a wave of firings all over the country, as companies are told their workers have invalid numbers, sparking fear that some of them may be illegal immigrants. **Sitting on $345 billion in uncredited money paid into the system, the government last year began sending letters to every company in America with at least one employee whose name did not match his or her Social Security number. The plan was intended to clear up misspellings, name changes, and other errors that might cause legitimate employees to drop out of the Social Security database. But the impact has fallen far more heavily on illegal immigrants, many of whom apply for jobs with false numbers.** Based on information from dozens of immigrant rights groups, the National Immigration Law Center, a policy and advocacy organization, estimates

thousands of workers across the country were fired last year after their names appeared on the government's "no−match" letters. **Josh Bernstein, the center's senior policy analyst, said, "The problem is that employers don't understand what it's about. They assume it's for immigration enforcement."**
Source: http://www.boston.com/dailyglobe2/077/metro/US_check_leads_to_wave_of_firings+.shtml

31. *March 17, Government Executive* — **Online security clearance system to debut in June.** An automated system to streamline security clearances and background checks for federal workers will be up and running by June, the Office of Personnel Management said Monday. **When complete, the e−clearance system will allow federal employees to update online the government form for national security positions. The online filing system will save workers time because it will let them use a two−page form−the SF−86C−to renew their applications, instead of a 13−page form every time their situation changes.** The SF−86C form has been designed, approved and is available for workers to use, but they cannot file the form electronically yet. Technology known as e−QIP, which is in its final testing phase, will make electronic filing possible. E−QIP will be ready for governmentwide use by June, according to Dan Blair, deputy director of OPM. **E−clearance, one of the 24 e−government initiatives supported by the president's management agenda, also includes the Clearance Verification System, which will allow agencies to access the results of background investigations or view clearance forms by searching in a single database.**
Source: http://www.govexec.com/dailyfed/0303/031703a1.htm

32. *March 17, Government Executive* — **Justice IG says foreign student tracking system inadequate.** The Internet−based system for tracking foreign students studying in the United States has "significant deficiencies," according to a report released Monday by the Justice Department's Office of the Inspector General. **The report found that the Immigration and Naturalization Service (INS) processes for certifying schools and training employees on the Student and Exchange Visitor Information System (SEVIS) are inadequate. Particular problems lie in INS' oversight of contractors hired to review the schools and in the reviews of schools' record−keeping and internal controls. It also noted that the SEVIS database will not include information on all foreign students until Aug. 1. Schools were required to begin using SEVIS for new foreign students first by Jan. 30 and later by Feb. 15, but have until August to enter information about continuing foreign students. "Until then, the INS will continue to operate its inadequate, paper−based system to monitor continuing foreign students," the report said.** In addition, INS has not established procedures to use SEVIS to identify potential fraud. The report includes eight recommendations to improve the system. Report: http://www.justice.gov/oig/inspection/I−2003−003/final.pdf
Source: http://www.usdoj.gov/oig/inspection/I−2003−003/final.pdf

[Return to top]

Emergency Services Sector

Nothing to report.
[Return to top]

Information and Telecommunications Sector

33. *March 18, Federal Computer Week* — **Army Web server hacked. A hacker last week exploited a previously unknown vulnerability in Microsoft Corp.'s Windows 2000 operating system to gain control of an Army Web server**. Russ Cooper of security services company TruSecure Corp. said that **on March 10 the hacker used an attack code to operate the Army system as if he or she had the highest security clearance and therefore was able to gain complete control of the system**. The Army identified the problem after performing a network scan and finding data output from a port on one of its internal servers to an "unspecified region," he said. Both Microsoft and Carnegie Mellon University's CERT Coordination Center issued security warnings about the "buffer overflow" vulnerability and Microsoft has developed a patch, available on the Microsoft Web site, to fix it. **The vulnerability affects systems running Microsoft Windows 2000 with Internet Information Server (IIS) 5.0 enabled and the code exploits an unchecked buffer in the WebDAV protocol. Exactly which Army computer was attacked, the sensitivity of the data contained on the system, and the attacker's intentions are still unknown**. Compounding the surprising nature of an attack on a Defense Department system is the fact that this was a previously unknown vulnerability, or "zero−day exploit," which are extremely rare in the computer security arena. Vendors often issue patches before hackers have infiltrated a system.
Source: http://www.computerwire.info/brnews/5C4592250BC485B508256CED 0003C976

34. *March 18, Government Computer News* — **DHS warns about systems threats as war looms. The Department of Homeland Security (DHS) on Tuesday reminded Internet users to be vigilant for cyberattacks in light of the ultimatum President Bush issued Monday** that Iraqi President Saddam Hussein leave his country or face military invasion. **The department and other federal agencies are monitoring "the Internet for signs of a potential terrorist attack, cyberterrorism, hacking and state−sponsored information warfare**," a Homeland Security statement said. "Industry and public Internet users are reminded of the importance of employing sound security practices and reporting unusual activity or intrusion attempts to DHS or local law enforcement."
Source: http://www.gcn.com/vol1_no1/daily−updates/21419−1.html

35. *March 17, CNET News.com* — **Linux firms urge users to plug Samba hole.** The open−source community is urging customers to patch their systems to close a hole in a software component that allows Windows programs to store and retrieve files on Linux and Unix servers. Known as Samba, the software can be found on many workstations and servers running any one of the variety of flavors of Linux and Unix, including systems running Apple OS X. **The flaw occurs in the code that reassembles data that the software receives from the Internet, according to the advisory. By sending the server a specially crafted data packet, an attacker could overload the memory used by the Samba software and cause the application to run code of the intruder's choice**. Members of the Samba team planned to announce the vulnerability on Tuesday, but they released information over the weekend because some believed a Web site break−in in Germany may have been attributed to the software. **Several Linux editions−−including Debian, Gentoo, and SuSE−−released patches for the problem. Apple Computer noted in an advisory that Samba is not enabled by default with Mac OS X and Mac OS X Server, but the company plans to issue a patch for version 10.2.4. Red Hat hasn't yet released a patch but will do so soon**, the company said in a statement.

Source: http://news.com.com/2100−1002−992965.html?tag=fd_top

36. *March 17, eWEEK* — **More net attacks loom, CERT says. The recent rash of Internet worms has produced an army of hundreds of thousands of compromised machines that could ultimately be used to launch a massive distributed−denial−of−service attack at any time**, according to security officials. Officials at the CERT Coordination Center said the organization is monitoring at least five large networks of compromised machines installed with so−called bots. **The bots connect compromised PCs or servers to Internet Relay Chat servers, which attackers commonly use to execute commands on the remote systems. At least one of these networks has more than 140,000 machines**, officials said. CERT's dire warning is underscored by last week's emergence of the Deloder and Code Red.F worms. **While neither worm does any immediate damage to infected machines, both install back doors that enable attackers to use compromised machines for future, much more damaging operations, such as DDoS attacks**. At the heart of this new trend, according to security experts, are poor security practices. But more important is the mistaken belief by corporate IT that once crises such as those caused by Code Red or SQL Slammer die down, the trouble's over. In fact, **after an initial flurry of advisories, warnings and patches, there are often months or years of sustained infections and residual DDoS attacks**, Marty Lindner of CERT said. **Also problematic are the many affected machines belonging to home users, few of whom do any logging of the activity on their PCs**. As a result, attackers can easily hide their tracks by using these anonymous computers, according to the experts.
Source: http://www.eweek.com/article2/0,3959,935790,00.asp

37. *March 17, eWEEK* — **Deloder, Lovgate worms mark perils of slack security policy. Many computer users persist in using their names or children's birthdays as log−on credentials**, and two recent worm outbreaks have shown why that's such a risky practice. **Deloder, the latest worm to hit vulnerable Windows machines, as well as a recent version of Lovgate, both use a list of common passwords in an attempt to compromise computers**. Lovgate began spreading late last month, while Deloder appeared last week. **Although neither worm has spread as far or as fast as threats such as SQL Slammer or Code Red, both Deloder and Lovgate clearly illustrate the danger inherent in lax security policies**. In Deloder's case, the worm tries to connect to random Windows NT, Windows 2000 and Windows XP machines on TCP port 445, normally used by Microsoft Corp.'s Active Directory. It then looks for network shares on the remote machine and, if it finds any, tries to copy itself to the shares by using easily guessed passwords to gain access. **The worm also installs a Trojan horse and a utility for executing commands on remote machines. Lovgate behaves in a similar fashion**. It spreads from an infected machine using the Messaging API Windows functions by answering recent mail with an infected reply. It then tries to copy itself to network shares and their sub−folders. If the folders are password− protected, Lovgate tries passwords such as "admin" and "123."
Source: http://www.eweek.com/article2/0,3959,936327,00.asp

Internet Alert Dashboard

Current Alert Levels

 AlertCon: 2 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_KLEZ.H** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	80 (www), 137 (netbios−ns), 1434 (ms−sql−m), 113 (ident), 445 (microsoft−ds), 25 (smtp), 139 (netbios−ssn), 53 (domain), 4662 (eDonkey2000), 0 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

38. *March 18, Washington Post* — **Demonstrators use more active tactics.** Unlike Saturday's antiwar march in Washington that drew tens of thousands, Monday's protest emphasized not large numbers but planned arrests. So at 11 a.m., after a rally at a Southeast Washington church and a march down Pennsylvania Avenue to the Capitol, the first three of dozens of protesters took a few steps into a restricted zone on the lawn and were placed under arrest. **The demonstration kicked off a weeklong series of rallies and acts of civil disobedience targeting Congress. Organizers estimated the crowd at 250. Capitol Police said 54 protesters were arrested. They included college students from North Carolina and Wisconsin, three physicians and a Catholic priest from New York, organizers said. Source: http://www.washingtonpost.com/wp−dyn/articles/A42464−2003Mar 17.html**

[Return to top]

DHS/NIPC Products &Contact Information

The Department of Homeland Security's National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The DHS/NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web−site (http://www.nipc.gov), one can quickly access any of the following DHS/NIPC products:

DHS/NIPC Warnings − DHS/NIPC Assessements, Advisories, and Alerts: DHS/NIPC produces three levels of infrastructure warnings which are developed and distributed consistent with the FBI's National Threat Warning System. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/NIPC Publications − DHS/NIPC Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/NIPC Daily Reports Archive − Access past DHS/NIPC Daily Open Source Infrastructure Reports

DHS/NIPC Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/NIPC Daily Report Team at 202−324−1129
Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information.

Contact DHS/NIPC

To report any incidents or to request information from DHS/NIPC, contact the DHS/NIPC Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/NIPC Disclaimer